



Department of Homeland Security Daily Open Source Infrastructure Report for 09 July 2007

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- Immigration and Customs Enforcement officials say increased immigration enforcement — such as the June raid at a produce plant in North Portland, Oregon — has pushed some undocumented workers to shift from fictitious Social Security numbers and green cards to identity theft. (See item [6](#))
- Investigators in the United States and Britain say three British residents who pleaded guilty to using the Internet to incite murder used computer viruses and stolen credit card accounts to set up a network of communication forums and Websites to further global jihad. (See item [8](#))

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *July 05, New York Times* — **Secrecy at nuclear agency is criticized by lawmakers.** Secrecy by the Nuclear Regulatory Commission (NRC) is now coming under attack by influential members of Congress. These lawmakers argue that the agency is withholding numerous documents about nuclear facilities in the name of national security, but that many withheld documents are not sensitive. The lawmakers say the agency must rebalance its penchant for secrecy with the public's right to participate in the licensing process and its right to know about potential hazards. Additional details of a hazardous spill in 2006 at a factory that makes

uranium fuel for nuclear reactors are coming to light now because of a letter sent Tuesday, July 3, to the nuclear agency by the House Energy and Commerce Committee. The letter says the commission “went far beyond” the need to protect security information by keeping documents about Nuclear Fuel Services, a private company, from the public. With a resurgence of nuclear plant construction expected after a 30-year hiatus, agency officials say frequently that they are trying to strike a balance between winning public confidence by regulating openly and protecting sensitive information. A commission spokesperson, Scott Burnell, said the “official use only” designation was under review.

Source: http://www.nytimes.com/2007/07/06/us/06nuke.html?_r=1&oref=s_login

2. *July 05, 600 Action News (Canada)* — **Canadian nuclear regulatory agency downplays threat of missing devices.** The Canadian Nuclear Safety Commission (CNSC) says it's not worried that radioactive devices that have gone missing in Canada during the past five years will be turned into crude nuclear weapons. Gerry Frappier, the Director General of the Directorate of Security and Safeguards, says the CNSC is very vigilant about the radioactive devices it licences, and monitors their use very closely. Frappier says only about 30 of the devices that were stolen or lost remain missing. Frappier says the Commission doesn't consider the threat very high, and adds there is no indication terrorist groups are responsible for the taking any of the devices.

Source: http://www.saskatoonhomepage.ca/index.php?option=com_ezine&task=read&page=9&category=21&article=6299&Itemid=86

3. *June 29, Pepco* — **Pepco completes new 230-KV lines, improves reliability for Washington, DC.** Pepco has placed into service two newly constructed high-voltage transmission lines that will enhance the reliability of electric service for downtown Washington, DC, and the federal government. The lines, each carrying 230,000 volts, were constructed over an 18-month period with completion in time to meet this summer's peak demand period. Pepco accelerated construction of these new transmission facilities in September 2005 following the shutdown of the Potomac River Generating Station in Alexandria, VA, by its owner, Mirant Corporation, in response to an environmental study. The plant, which was reopened under an emergency order from the U.S. Department of Energy, played a critical role in backing up transmission lines serving District customers prior to construction of the new lines. The plant continues to provide support for the regional power grid. The new lines run underground through two pipes a distance of 5.6 miles, connecting a high-voltage transmission substation in Prince George's County with a substation near the District. To install the lines, Pepco installed more than 11 miles of special pipes and heavily upgraded the two substations.

Source: <http://www.pepco.com/welcome/news/releases/archives/2007/article.aspx?cid=817>

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

4. *July 05, U.S. Department of Defense* — **DoD officials offer \$1 million prize for wearable power innovations.** A typical dismounted troop going out for a four-day mission carries as much as 40 pounds of batteries and rechargers in his pack. Department of Defense (DoD) officials want to reduce that load significantly, and they're dangling a \$1 million carrot to entice people to help them do it. They launched their "wearable power" prize competition Thursday, July 5, to come up with new innovations to lighten warfighters' loads. The goal, explained William Rees, deputy undersecretary of laboratories and basic sciences, is to reduce the weight for the power system that drives radios, night-vision devices, global positioning systems and other combat gear, including a recharging system, to about two pounds per day. Competitors have until November 30 to register for the competition.

Source: <http://www.defenselink.mil/news/newsarticle.aspx?id=46643>

5. *July 05, Federal Computer Week* — **Report: Congress needs to take charge of DoD procurement policy.** Congress needs to take a stand before the Department of Defense (DoD) sets a new procurement precedent and moves away from a decades-old policy of paying for a project with one fiscal year's appropriations. But the question for Congress is how to do that, according to a new Congressional Research Service (CRS) report. Current policy requires DoD to fund a weapon or piece of equipment in the year in which the item is bought. The full-funding policy is a budgeting rule that has been applied to DoD procurement programs since the 1950s. Ronald O'Rourke and Stephen Daggett, national defense specialists in CRS' Foreign Affairs, Defense and Trade Division, wrote in the report that despite being a technical rule, the policy deals with Congress' budget power and oversight of DoD. "The issue for Congress is how to respond to DoD's proposals for procuring ships and aircraft...with funding approaches that do not conform to the full-funding policy," they wrote. "Congress' decision on this issue could have significant implications for Congress' ability to conduct oversight of DoD procurement programs." They added that it also could affect how DoD budgets its annual funding requirements.

CRS Report: <http://www.fas.org/sgp/crs/natsec/RL31404.pdf>

Source: <http://www.fcw.com/article103157-07-05-07-Web>

[\[Return to top\]](#)

Banking and Finance Sector

6. *July 06, Associated Press* — **Illegal workers turn to ID theft.** Fictitious Social Security numbers and green cards are cheap and widely available, and getting them is the first step for many undocumented immigrants arriving in Oregon. But workers and federal officials say increased immigration enforcement — such as June's raid at a produce plant in North Portland and the detention of 167 workers — has pushed some undocumented workers to shift from forgery to identity theft. "Enforcement is deterring people, but it's also having another effect," said Kevin Sibley of U.S. Immigration and Customs Enforcement. "Aliens are finding it more difficult to find jobs using the traditional counterfeit documents. So they're willing to commit the extra step to beat the system and get a job. The next step is using someone else's identity." During one stretch last year, American Staffing Resources — which supplied temporary workers to the Fresh Del Monte plant — employed 596 workers there, of whom 463, about 78 percent, were using someone else's Social Security number. Only 48 employees had valid,

matching Social Security numbers. Federal authorities attribute the proliferation of fraudulent documents to a rise in multinational criminal organizations branching out into the documents market and the misuse of Social Security numbers by employees.

Source: <http://159.54.226.83/apps/pbcs.dll/article?AID=/20070706/STA/TE/707060333&template=printart>

7. *July 06, Register (UK)* — **Turing test challenges spam filters.** Spammers have turned a widely-used anti-spam trick — fuzzy text that computers cannot recognize — to their own advantage, according to the head of an anti-spam software developer. The distorted text images are arriving in PDF files touting German penny stocks, in yet another iteration of the pump-and-dump scam that's been around for a while now. What's different from earlier image spam is not only that these are PDFs, which adds an extra layer of complexity to the task of filtering out spam, but the text inside is deliberately distorted to make it extra-hard for computers to recognise. Neil Cook of Cloudmark, called it "a kind of Turing test for spam filters." He then added, "We've been seeing a lot of PDF stock spams for the last 10 days or so, and there was another spike last night. Images are particularly easy for humans to pick up, but particularly hard for computers.

Source: http://www.channelregister.co.uk/2007/07/06/fuzzy_image_spam/

8. *July 06, Washington Post* — **Three worked the Web to help terrorists.** The global jihad landed in Linda Spence's e-mail inbox during the summer of 2003, in the form of a message urging her to verify her eBay account information. She clicked on the link included in the message, which took her to a counterfeit eBay site where she entered personal financial information. Spence's information wound up in the hands of a man in Britain who was the brains behind a cell that sought to facilitate bombings in the United States, Europe, and the Middle East. Spence's stolen data made its way via the Internet black market for stolen identities to a biochemistry student, Tariq al-Daour, one of three British residents who pleaded guilty this week to using the Internet to incite murder. The British investigation revealed a significant link between Islamic terrorist groups and cyber-crime. Investigators in the United States and Britain say the three used computer viruses and stolen credit card accounts to set up a network of communication forums and Websites that hosted such things as tutorials on computer hacking and bomb-making, and videos of beheadings and suicide bombings in Iraq.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501945.html>

9. *July 05, Government Accountability Office* — **GAO-07-737: Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (Report).** The Government Accountability Office (GAO) was asked to examine (1) the incidence and circumstances of breaches of sensitive personal information; (2) the extent to which such breaches have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements. To address these objectives, GAO reviewed available reports on data breaches, analyzed 24 large data breaches, and gathered information from federal and state government agencies, researchers, consumer advocates, and others. While comprehensive data do not exist, available evidence suggests that breaches of sensitive personal information have occurred frequently and under widely varying circumstances. The extent to which data breaches have resulted in identity theft is not well known, largely because of the difficulty of determining the source of

the data used to commit identity theft. However, available data and interviews with researchers, law enforcement officials, and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft, particularly the unauthorized creation of new accounts. Should Congress choose to enact a federal notification requirement, use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications of breaches that present little risk.

Highlights: <http://www.gao.gov/highlights/d07737high.pdf>

Source: <http://www.gao.gov/docsearch/abstract.php?rptno=GAO-07-737>

10. *July 03, Sophos* — **Criminal investigation secrets, student records leak onto Internet by peer-to-peer file-sharing networks.** According to SophosLabs, media reports have revealed that sensitive information has been leaked onto the Internet from virus-infected computers. The Metropolitan Police Department in Tokyo has confirmed that personal information about 12,000 people related to criminal investigations has been distributed across the Net from an officer's infected computer. The police officer, who had installed the Winny file-sharing software on his PC, did not realize that a piece of malicious code was making the confidential data available to other users via the peer-to-peer network. About 6,600 police documents are said to have been compromised, including interrogation reports, statements from victims of crime, and classified locations of automatic license plate readers. Coincidentally, it was also revealed that almost 15,000 pieces of personal information about students was leaked onto the Internet from a PC belonging to a high school teacher in Ichinomiya. The teacher, who was running the Share P2P file-sharing program, had also been compiling a list of retired Air Self-Defense Force officers on behalf of his mother who had worked at their base in Kagamihara. This information also leaked onto the Internet. These are not the first occasions that malware has taken advantage of peer-to-peer file-sharing networks to steal information. Source: <http://www.sophos.com/pressoffice/news/articles/2007/07/jp-secrets.html>

[\[Return to top\]](#)

Transportation and Border Security Sector

11. *July 08, Associated Press* — **New York City tour copter plunges into river.** A Eurocopter EC-135 helicopter on a sightseeing tour of Manhattan made an emergency landing in the Hudson River on Saturday afternoon, July 7, leaving all eight people aboard drenched but not seriously harmed, authorities said. The seven passengers and a pilot were pulled from the waters between Manhattan and New Jersey by two Good Samaritan vessels as smoke poured from the bobbing aircraft. It appeared the helicopter had engine trouble before it went down, passengers said. The pilot deployed yellow emergency floats and made a controlled landing, authorities said. The propellers were askew, but the aircraft, which was owned by Liberty Helicopters, did not appear badly damaged, according to Federal Aviation Administration (FAA) spokesperson Holly Baker. The rescuers passed the eight to Coast Guard officials, who returned them to shore for medical evaluation, Fire Department spokesperson Craig Mosia said. There were no serious injuries, the Coast Guard said. The FAA planned to investigate, Baker said. Liberty Helicopters, which runs sightseeing excursions around the Statue of Liberty, Ellis Island, and Manhattan, said it had no comment.

Source: http://hosted.ap.org/dynamic/stories/H/HELICOPTER_DOWN?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

12. *July 06, USA TODAY* — **Travelers told to expect delays all summer at UK airports.** Prime Minister Gordon Brown on Friday, July 6, warned travelers to expect delays at Britain's airports throughout the summer. His warning that delays could run through the busy tourist season comes after the government earlier this week imposed new restrictions following the failed car-bomb attack on Scotland's Glasgow Airport. Cars and taxis are banned from picking up or dropping off passengers close to the terminals at most of Britain's airports. "Crowded places and airports, I think people will have to accept that the security has got to be more intense," Brown said. "We have got to avoid the possibility that people can use these crowded places for explosions." On June 30, two men rammed an SUV packed with gasoline and gas canisters into a departure terminal at Glasgow Airport. The attempted terror attack came a day after police defused two car bombs left to explode outside nightclubs in London's busy West End.

Source: http://www.usatoday.com/travel/flights/2007-07-06-uk-airport-delays_N.htm

13. *July 05, Canadian Press* — **Group urges U.S. to stop baggage re-screening.** The Canadian Airports Council is calling on the United States to stop the practice of re-screening luggage originating at Canadian airports. The council says the re-screening, in place since the 9/11 terrorist attacks, is unnecessary and adds to the travel times for trans-border travelers. It says Canada implemented baggage screening protocols in line with those introduced in the U.S. and other parts of the world after the attacks. But six years after 9/11, says the council, the U.S. does not recognize Canadian standards and re-screens bags from Canadian airports before allowing them onto connecting flights. The council has called on Prime Minister Stephen Harper and U.S. President George Bush to discuss this "critical issue" when they meet August 20th and 21st in Montebello, Quebec.

Source: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20070705/baggage_screen_070705/20070705?hub=Canada

[[Return to top](#)]

Postal and Shipping Sector

Nothing to report.

[[Return to top](#)]

Agriculture Sector

14. *July 06, USAgNet* — **Scam aimed at farmers selling hay online.** Missouri Attorney General Jay Nixon says hay farmers are the targets of a new Internet scam aimed at Missouri's agriculture community. The Missouri Department of Agriculture offers a Hay Directory on its Website where farmers register to advertise and sell their hay. Nixon says con artists are contacting businesses registered on the Website, in hopes of tricking them out of hundreds or even thousands of dollars. In this case, the hay seller receives an e-mail from someone claiming to be a hay buyer. The seller then receives a large check and is asked to wire money to a hauler, who will supposedly come and pick up the bales. The technique is a variation of the overpayment scam, where the con artist mails a check to the seller, then asks the seller to send part of that money elsewhere via wire transfer. The seller then finds out some days or weeks

later that the original check has bounced.

Source: <http://www.usagnet.com/story-national.php?Id=1557&yr=2007>

[\[Return to top\]](#)

Food Sector

15. *July 06, CNN* — **Massachusetts issues tainted toothpaste warning.** The Massachusetts Department of Public Health issued an advisory Friday, July 6, the same day Panama announced that hundreds of poisoning cases were linked to diethylene glycol. Massachusetts warned consumers to not use the following potentially harmful toothpastes: Any toothpaste labeled "Made in China," Any toothpaste labeled "Colgate" that is manufactured in South Africa, And any toothpaste without English-language labeling. The warning came on the same day that officials in Panama said they had recorded 540 cases of poisoning linked to toothpaste and other health products in that country. Dimas Guevara, a special Panamanian prosecutor, said 83 deaths had been linked to diethylene glycol, a chemical used in antifreeze, which was in the products.
Source: <http://money.cnn.com/2007/07/06/news/toothpaste/>
16. *July 04, Associated Press* — **Seasoning on snacks found tainted with salmonella.** A seasoning made with imported Chinese ingredients used on recalled snack foods was contaminated with salmonella, a company executive said Tuesday, July 3. The snack foods sickened dozens of people. The seasoning, used on Super Veggie Tings Crunchy Corn Sticks and Veggie Booty snack foods, tested positive for the bacteria, said Robert Ehrlich, chief executive of Robert's American Gourmet Food Inc. The "veggie" seasoning's ingredients came primarily from China, the company said. Veggie Booty was recalled last week after it was associated with 54 cases of salmonella poisoning in 17 states. The company expanded the recall Monday to include Super Veggie Tings Crunchy Corn Sticks because it used the same seasoning.
Source: <http://www.latimes.com/business/la-fi-booty4jul04.1,6631822.story?coll=la-headlines-business>
17. *July 04, Associated Press* — **Explosion at Wichita Cargill plant sparks a fire.** An explosion at a Cargill facility on Wednesday, July 4, in Wichita, KS, sparked a fire and prompted the closing of several blocks around the plant. Wichita fire marshal Ed Bricknell said no secondary explosions were expected. However, the fire continues to smolder because damage to the building prevented firefighters from getting to the source.
Source: http://www.kansascity.com/news/breaking_news/story/177135.htm
18. *July 02, U.S. Food and Drug Administration* — **FDA and EFSA strengthen cooperation in food safety science.** The European Food Safety Authority (EFSA) and the U.S. Food and Drug Administration (FDA) Monday, July 2, signed the first U.S./European agreement in the area of assessing food safety risk. This is the first formal international cooperation agreement EFSA has signed and the first formal step in cooperation between the two bodies. The agreement is designed to facilitate the sharing of confidential scientific and other information between EFSA and the FDA, such as methodologies to ensure that food is safe. A formal agreement ensures

appropriate protection of such confidential information under the applicable legal frameworks in both the United States and the European Union. Informal cooperation and dialogue have already been established between the two bodies; this agreement will enable these to be formalized and extended.

Source: <http://www.fda.gov/bbs/topics/NEWS/2007/NEW01664.html>

[\[Return to top\]](#)

Water Sector

Nothing to report.

[\[Return to top\]](#)

Public Health Sector

19. *July 07, Atlanta Journal Constitution* — CDC lab's backup power fails during storm. A lightning strike knocked out power for about an hour last month at the U.S. Centers for Disease Control and Prevention's (CDC) new \$214 million infectious disease building — including the agency's six high — tech labs that will soon handle the world's most deadly germs. Backup power did not come on. The suite of Biosafety Level 4 labs, designed to contain the likes of Ebola and avian influenza, was unoccupied during the June 15 outage. While the incident also affected the labs' air pressure safety system, CDC officials on Friday, July 6, emphasized that even if the labs had been in use, the agency's staff and the public would never have been in any danger because of the building's many containment systems. Last month's power outage revealed an issue with how the new building handles power surges and has engineers considering whether to route a special backup power supply to the BSL-4 labs, said George Chandler, who is in charge of building and facilities at CDC.

Source: <http://www.ajc.com/news/content/metro/dekalb/stories/2007/07/06/0707meshcdclab.html>

20. *July 06, Agence France–Presse* — Bird flu spreads to poultry in Germany. The H5N1 bird flu virus has spread to poultry in Germany after killing dozens of wild birds in the past fortnight, the national veterinary laboratory said on Friday, July 6. The virus infected a goose on a small holding in a forest near Wickersdorf in the eastern state of Thuringen where the owner kept four other geese and five ducks, the Friedrich Loeffler Institute said. It is the first time this year that the highly pathogenic strain of avian flu, which can also kill humans, was found among domestic birds in Germany. It has infected wild birds in Thuringen and three other German states since late June. The Friedrich Loeffler Institute said 153 wild birds found dead this week on the shores of an artificial lake on the border of Thuringen had all tested positive for H5N1 bird flu.

Source: http://news.yahoo.com/s/afp/20070706/hl_afp/healthflugermany_070706184200;_ylt=AslvAEoW6GIVp3NsKSLJytCJOrgF

21. *July 05, Minnesota Public Radio* — States and Ontario to share infectious disease information. Several U.S. states and the Canadian province of Ontario have formally agreed to share information about infectious diseases. It gives public health officials contact information,

and a protocol for how quickly to call, when a disease shows up that might affect people in different places. The Minnesota Department of Health's Steve Shakman says if a person gets sick while they're away from home, they'll have a better chance of getting quick and effective treatment. In addition to Minnesota and Ontario, the agreement covers Wisconsin, Michigan, and New York.

Source: <http://minnesota.publicradio.org/display/web/2007/07/05/diseasinfo/>

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

22. *July 07, Federal Emergency Management Agency* — President declares major disaster for Oklahoma. The head of the U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) announced Saturday, July 7, that federal disaster aid has been made available for the state of Oklahoma to supplement state and local recovery efforts in the area struck by severe storms, flooding and tornadoes during the period of June 10, 2007, and continuing. FEMA Administrator David Paulison said the assistance was authorized under a major disaster declaration issued for the state by President Bush. The President's action makes federal funding available to affected individuals in Ottawa and Washington counties.

Source: <http://www.fema.gov/news/newsrelease.fema?id=37649>

23. *July 07, Asbury Park Press (NJ)* — New command center has New Jersey prepared. A vehicle providing a cutting edge emergency communications system was unveiled in New Jersey on Friday, July 6: A new joint Mobile Command and Training Truck designed by the Monmouth University Center for Rapid Response Database Systems and Homeland Intelligence Technologies. The truck boasts a computer system that can connect computer databases at New Jersey pharmacies, hospitals, nursing homes, schools, and veterinary offices. It should also be able to detect spikes and other patterns in symptoms of emergency room patients, medicines purchased at drug stores, reasons for children missing school, even what illnesses veterinarians are treating pets for, because symptoms of some illnesses show up first in animals. The truck will be used as a command center and for gathering information and intelligence that could be used to channel resources and responses to a biological terrorist attack, disease outbreak, or natural disaster. The university's rapid response center works with the military to develop a coordinated communications system that will allow local, county, regional, state and federal agencies to exchange information and thus respond more effectively to a biological or chemical attack, disease outbreak, or a natural disaster.

Source: <http://www.app.com/apps/pbcs.dll/article?AID=/20070707/NEWS01/707070445/1004/NEWS03>

24. *July 06, Southwest Nebraska News* — Nebraska State Patrol logs on new safety tool. A new state-of-the-art Computer Aided Dispatch (CAD) system is on-line at the Nebraska State

Patrol. The \$1.1 million CAD system provides the latest computer technology to assist with receiving, managing and dispatching emergency calls statewide. The new system automates the Nebraska State Patrol's manual dispatch operations allowing dispatchers to respond to, manage, and track emergency calls more efficiently. The Windows based system, networks the Nebraska State Patrol's six troop area emergency communications centers to share calls and resources and provide remote backup capabilities. Since all data is duplicated at each site, in the event one of the Patrol's six communication centers becomes inoperable another center can resume full operation with accurate, up-to-the-minute information.

Source: http://www.swnebr.net/newspaper/cgi-bin/articles/articlearch_iver.pl?161335

[[Return to top](#)]

Information Technology and Telecommunications Sector

25. *July 06, Reuters* — **Norwegian hacker says he can bypass AT&T on iPhone.** A well-known hacker claims to have overcome restrictions on Apple Inc.'s iPhone, allowing highly technical users to bypass AT&T Inc.'s network to use the phone's Internet and music features. In a post dated Tuesday, July 3, on his blog, Jon Johansen, 23, a prolific hacker of consumer electronics gadgets since he was a teenager in Norway, said "I've found a way to activate a brand new unactivated iPhone" without signing up for AT&T service. "The iPhone does not have phone capability, but the iPod and Wi-Fi work. Stay tuned!" he wrote on his long-running blog, which is combatively named "So Sue Me." The site contained technical details for other hackers, as well as links to software necessary to complete the process.

Source: <http://www.eweek.com/article2/0.1895.2155284.00.asp>

26. *July 06, VNUNet* — **Trojan uses Hotmail and Yahoo as spam hosts.** Security firm BitDefender has warned of a new e-mail threat using Hotmail and Yahoo Mail accounts to send spam. Trojan.Spammer.HotLan.A uses automatically generated e-mail accounts, suggesting that spammers have found a way to bypass so-called Captcha systems. Captcha works by preventing new accounts being created until the creator correctly identifies the letters depicted in an image. Every active copy of the Trojan accesses an account, and pulls encrypted spam e-mails from a Website. It then decrypts the e-mails and sends them to valid addresses taken from yet another Website. "There are only about 500 or so new accounts being created every hour," said Viorel Canja, head of BitDefender's antivirus lab. "But we have seen at least 15,000 Hotmail accounts being used so far. It is hard to estimate how many spam e-mails have already been sent." The spam currently being distributed attempts to lure users to a site advertising pharmacy products.

Source: <http://www.vnunet.com/vnunet/news/2193671/trojan-hotmail-yahoo-spam-hosts>

27. *July 05, IDG News Service* — **Talking Trojan says 'bye bye' to victims' data.** A newly identified malicious program not only messes up its victims' computers, it taunts them too. The program, called the BotVoice.A Trojan was first spotted by security vendor Panda Software about two weeks ago. It is a Trojan horse program, which the victim must download first. But once installed, it gets nasty. The Trojan soon sets to work trying to delete everything from the victim's hard drive, while at the same time endlessly repeating an audible message, apparently designed to taunt the victim. "You have been infected; I repeat, you have been infected and your system files have been deleted. Sorry. Have a nice day and bye bye," the Trojan says. It

does this by using a text-reading program that is part of the Windows operating system, Panda said. Users of Windows 2003, XP, 2000, NT, ME, 98, and 95 are all at risk. Unlike a virus, BotVoice.A does not jump from computer to computer on its own, but spreads via peer-to-peer networks or storage devices such as CD-ROMs or USB memory drives.

Source: http://www.infoworld.com/article/07/07/05/Talking-Trojan-say-s-bye-to-data_1.html

28. *July 05, ComputerWorld* — **Mpack installs ultrainvisible Trojan.** The notorious Mpack hacker toolkit is installing malware that carries out its chores — including spewing spam — from within the Windows kernel, making it extremely difficult for security software to detect it, Symantec said Thursday, July 5. The Trojan horse that Symantec has dubbed "Srizbi" is being dropped onto some PCs by the multi-exploit Mpack, a ready-to-use attack application that until recently has been selling for around \$1,000. Responsibility for a large-scale attack launched from thousands of hijacked Websites last month was pinned on Mpack, as was a follow-up campaign waged from compromised Internet porn sites. Although Mpack can force-feed any malicious code to a commandeered PC, Symantec researchers said Srizbi stands out. Rather than follow the current practice of hiding only some activities with rootkit-cloaking technologies, Srizbi goes completely undercover. The new Trojan, said Symantec, works without any user-mode payload and does everything from kernel mode, including its main task: sending spam.

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026323&intsrc=hm_list

29. *July 05, Washington Technology* — **DHS cyber security IG report released.** The National Cyber Security Division of the Department of Homeland Security (DHS) needs to do a better job of establishing priorities for key programs and managing them effectively, according to a new inspector general (IG) report. Although the division has made progress since 2004 in achieving its mission of advancing the nation's cyber security, officials have not set strategic priorities nor set a detailed schedule for achieving them, states a report from DHS Inspector General Richard L. Skinner.

IG report: http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_07-48_Jun07.pdf

Source: http://www.washingtontechnology.com/online/1_1/30971-1.html?topic=homeland

30. *July 04, Register (UK)* — **Security consultant's blog found pushing crudware.** A prominent IT security consultant has issued a mea culpa after learning a blog he set up on Blogspot and later abandoned is being used to push crudware. "If I'm supposed to know what I'm doing, what about the 299 million people out there who don't know better?" said Winn Schwartau, an expert in information warfare and computer security education, when asked why his old security blog, SecurityAwareness, tries to trick visitors into installing crudware called Malware Alarm. The incident is a cautionary tale for anyone who has ever kept a blog or Website and then decided to pull the plug. Schwartau had ditched the Blogspot address for a new URL that was linked to the Website of The Security Awareness Company, a business he runs. A spokesperson for Google, which runs Blogspot, said when the URL was retired, it went back into regular rotation, meaning it was available for the first person to request it. The new owner, evidently, is responsible for the content that warns users they may have malware and invites them to download Malware Alarm.

Source: http://www.channelregister.co.uk/2007/07/04/security_blog_pushes_crudware/

31. *July 03, Federal Computer Week* — **IG finds FEMA's laptop security faulty.** The Federal Emergency Management Agency (FEMA) does not have effective procedures to protect information contained on its laptop computers, according to a new report from Richard Skinner, the Department of Homeland Security's inspector general (IG). The IG tested 298 of the 32,000 laptop computers FEMA has in its inventory and discovered shortcomings in the agency's ability to set security configurations, conduct patching to remedy vulnerabilities and manage its inventory. FEMA officials agreed with the IG's report.
IG Report: http://www.dhs.gov/xoig/assets/mgmttrpts/OIGr_07-50_Jun07.pdf
Source: <http://www.fcw.com/article103138-07-03-07-Web>

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

32. *July 06, KNTV (CA)* — **All-Star festivities bring thousands to San Francisco.** Those attending this year's Major League Baseball All-Star events in San Francisco can expect tight security and traffic restrictions according to the city's police department. Officers said there would be numerous traffic restrictions near AT&T Park during the games that start Friday, July 6, and end Wednesday, July 11. The ballpark security will consist of designated checkpoints where officials will be looking for restricted items and enforcing counterfeit regulations. Undercover investigators will be on the lookout for counterfeit merchandise at the park and the Moscone Center as well as at manufacturing facilities, retail stores and sidewalk vendors in San Francisco. Security at McCovey Cove/China Basin Channel will be implemented from Saturday to Tuesday and includes a zone in which only pre-screened official vessels, law enforcement and media vessels, and a limited number of human-powered watercrafts will be permitted. The extra security measures taken consist of law enforcement officials and security personnel watching the areas from Moscone West Convention Center and Piers 30 and 32 south to the AT&T Park vicinity, as well as the McCovey Cove/China Basin Channel area.
Source: <http://www.nbc11.com/news/13630826/detail.html>

33. *July 06, Associated Press* — **Five hurt in Vegas casino shooting.** A man on a balcony over the New York-New York casino floor opened fire on the gamblers below early Friday, July 6, wounding four people before he was tackled by off-duty military reservists, police said. A fifth person was hurt in a crush of people fleeing the casino. "It was crazy, pandemonium," said Jade Jacobson, 28, a tourist from Deland, FL, whose cousin, a dance teacher from Pennsylvania, was wounded in the leg. All the injuries were described as minor, and none of the victims remained hospitalized Friday morning, authorities said. Las Vegas police Capt. James Dillon said a woman and a teenage boy were wounded; a man was grazed by a bullet; a woman was hit by a bullet fragment or shrapnel; and a woman was bruised and scraped when she fell amid the

crowd of people exiting the casino. Steven Zegrean, 51, of Las Vegas, was arrested on felony charges including attempted murder, battery with a deadly weapon and discharging a firearm in an occupied structure, Dillon said.

Source: http://www.usatoday.com/news/nation/2007-07-06-vegas-shooting_N.htm

- 34. July 06, Associated Press — FBI probes threat to Goldman Sachs.** The FBI is investigating anonymous mailed threats against the Goldman Sachs investment firm but does not consider the warnings to be of "high credibility," an investigator said on Friday, July 6. The letters, handwritten in red ink on loose-leaf paper and signed "A.Q.U.S.A.," were mailed to 20 newspapers around the country, authorities said. The letters contained the warning: "Hundreds will die. We are inside. You cannot stop us." Michael DuVally, a Goldman Sachs spokesperson, said the firm was working closely with law enforcement authorities, adding that authorities told the firm they don't believe the threat is credible.

Source: http://blog.silive.com/advanceupdate/2007/07/fbi_probes_threat_to_goldman_s.html

[\[Return to top\]](#)

General Sector

- 35. July 08, Associated Press — Wildfires flare across the West.** An 8,000-acre wildfire forced hundreds of people in the town of Winnemucca, about 170 miles east of Reno, NV, to leave their homes, one of more than a dozen blazes that charred a combined 55 square miles in northern Nevada. Yet another Nevada fire that was started by lightning Saturday threatened structures and led to the evacuation of campers about 30 miles south of Elko, officials said. The blaze was among a series that dotted the West on Saturday, July 7, as a heat wave made parched terrain even drier, forcing authorities to evacuate homes and close highways and wilderness areas. The Utah fire, about 120 miles south of Salt Lake City, forced the evacuations of Cove Fort and the Blundell Geo Thermal Power Plant, where it was threatening railroad lines, bridges, and several homes, Color County Fire Information Officer LaCee Bartholomew said. Interstate 70 was also closed in Richfield, according to Utah Highway Patrol Lt. Steve Winward. A 100-mile stretch of Interstate 15 in central Utah was closed when a 160,000-acre wildfire jumped the highway, and other fires burned in California, Colorado, Arizona, Idaho, Oregon, and Washington.

Source: http://www.usatoday.com/news/nation/2007-07-08-wildfires_N.htm

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.